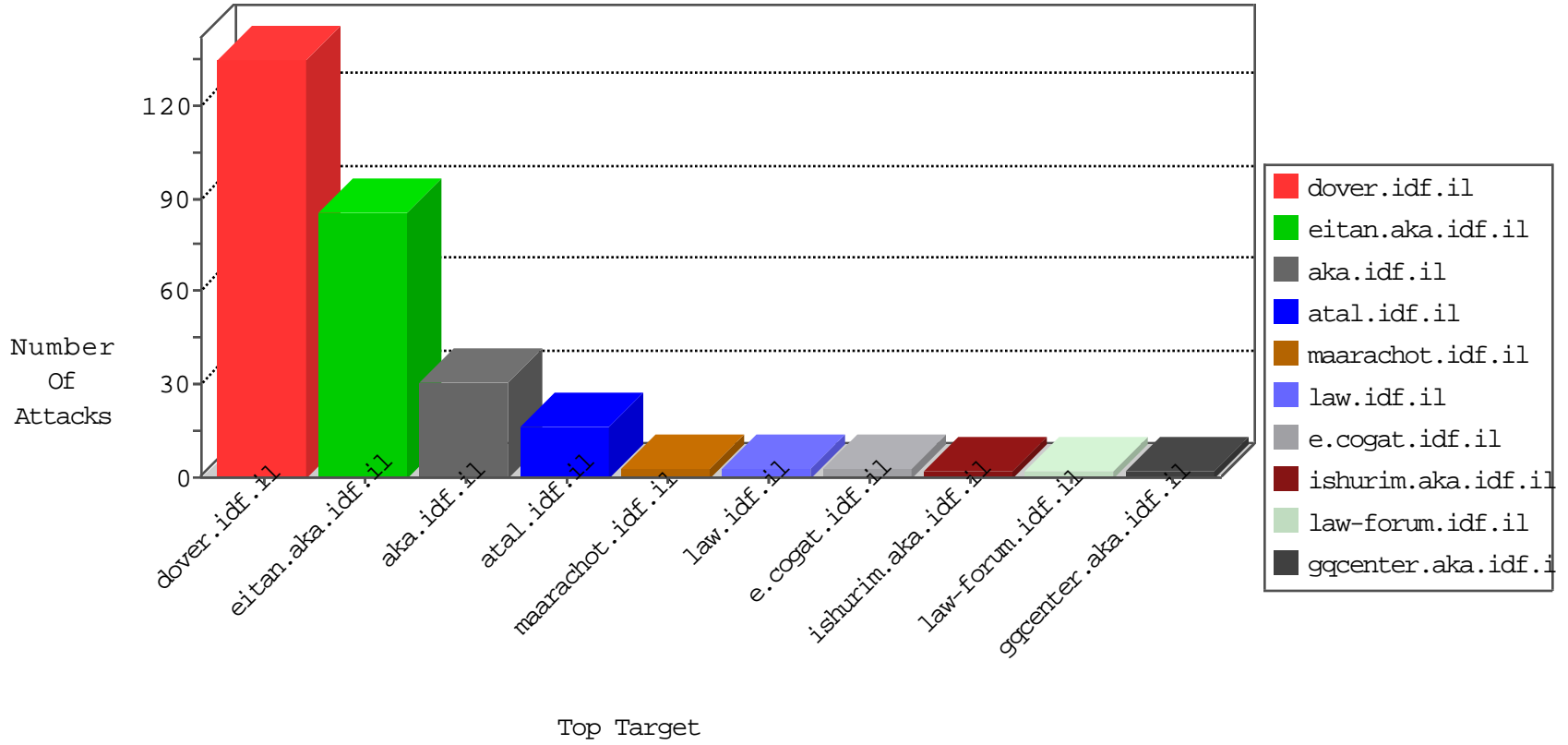


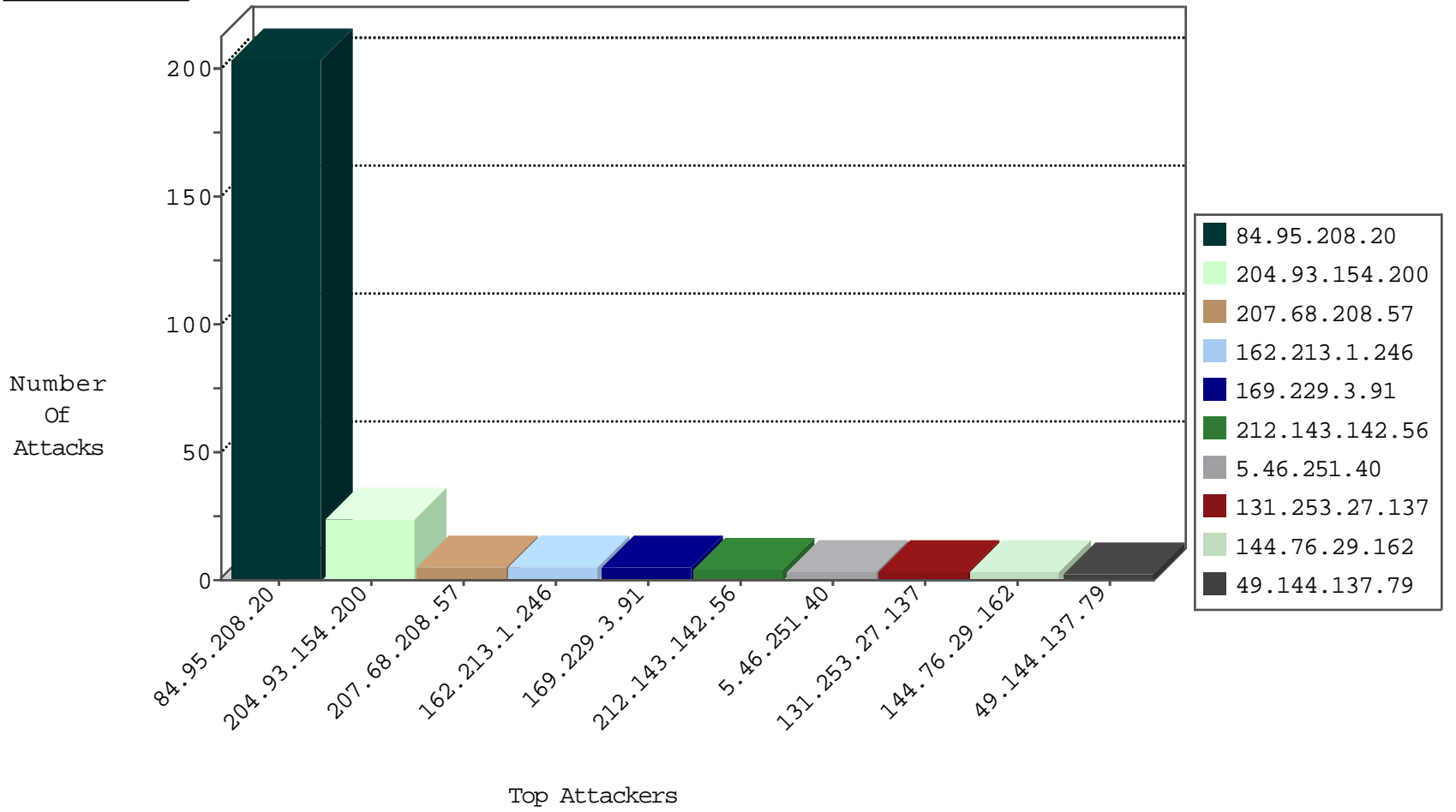
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
204.93.154.200	United States	147.237.72.166	aka.idf.il	TCP Scan (vertical)	drop	181
61.64.21.176	Taiwan	147.237.76.148	ggcenter.aka.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
109.65.82.9	Israel	147.237.72.167	ishurim.aka.idf.il	network flood IPv4 TCP-RST	drop	2
208.115.113.89	United States	147.237.72.166	aka.idf.il	network flood IPv4 TCP-RST	drop	1
43.225.205.2	Bangladesh	147.237.77.19	law-forum.idf.il	Invalid TCP Flags	drop	1
89.248.168.21	Netherlands	147.237.76.176	test.ncore.idf.il	Black List	drop	1
209.126.136.2	United States	147.237.76.201	e.atal.idf.il	Black List	drop	1
43.225.205.2	Bangladesh	147.237.77.61	e.cogat.idf.il	Invalid TCP Flags	drop	1
43.225.204.2	Bangladesh	147.237.77.19	law-forum.idf.il	Invalid TCP Flags	drop	1
43.225.206.2	Bangladesh	147.237.77.61	e.cogat.idf.il	Invalid TCP Flags	drop	1
43.225.204.2	Bangladesh	147.237.77.61	e.cogat.idf.il	Invalid TCP Flags	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
144.76.29.162	Germany	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Permit	3
199.58.86.209	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
80.240.139.111	Netherlands	147.237.77.216	dover.idf.il	24910: HTTP: Python urllib User-Agent Header	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
162.213.1.246	147.237.77.216	United States	dover.idf.il	Tehila - Perl LWP with fake user agent	5
46.120.122.219	147.237.77.170	Israel	maarachot.idf.il	Xenu Link Sleuth User Agent	2

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
49.144.137.79	Philippines	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
66.249.66.161	Israel	147.237.0.33	idf.il	drop		drop	1
169.229.3.91	United States	147.237.77.243	mobile.idf.il	drop	SAM rule	drop	1
169.229.3.91	United States	147.237.76.31	nakchal.idf.il	drop	SAM rule	drop	1
169.229.3.91	United States	147.237.76.147	chinuch.aka.idf.il	drop	SAM rule	drop	1
5.46.251.40	Turkey	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
169.229.3.91	United States	147.237.76.200	eitan.aka.idf.il	drop	SAM rule	drop	1
169.229.3.91	United States	147.237.77.234	halag.idf.il	drop	SAM rule	drop	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	101
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	84
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	8
84.95.208.20	Israel	147.237.77.233	atal.idf.il	PHP Attempt	Block	6
207.68.208.57	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/main/	Block	5
131.253.27.137	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	3
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
5.46.251.40	Turkey	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in www.idf.il/1065-en/dover.aspx	Block	2
84.95.208.20	Israel	147.237.77.216	dover.idf.il	PHP Attempt	Block	2
66.249.76.75	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
207.46.13.20	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/watch	Block	1
66.249.76.28	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
109.65.166.231	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/himush/site/he/himush.asp	Block	1
66.249.76.83	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.76.29	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/894-he/atal.aspx	Block	1
68.180.228.225	United States	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on list.ips.gov.il/robots.txt	Block	1
66.249.76.70	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.76.70	Block	1
194.153.113.35	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
66.249.66.177	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.76.70	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/apple-app-site-association	Block	1
199.30.17.49	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter tab in www.eitan.aka.idf.il/938-he/eitan.aspx	None	1
66.249.69.166	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/5/112745.pdf	Block	1